Release Notes for the Cisco ME 3400 Ethernet Access Switches, Cisco IOS Release 12.2(25)SEG and Later

Revised September 24, 2008

Cisco IOS Release 12.2(25)SEG and later run on the Cisco ME 3400 Series Ethernet Access switches.

These release notes include important information about Cisco IOS Release 12.2(25)SEG and later, and any limitations, restrictions, and caveats that apply to it. Verify that these release notes are correct for your switch:

- If you are installing a new switch, see the Cisco IOS release label on the rear panel of your switch.
- If your switch is on, use the **show version** privileged EXEC command. See the "Finding the Software Version and Feature Set" section on page 3.
- If you are upgrading to a new release or different image, see the software upgrade filename for the software version. See the "Deciding Which Files to Use" section on page 3.

For the complete list of Cisco ME 3400 switch documentation, see the "Related Documentation" section on page 27.

You can download the switch software from this site (registered Cisco.com users with a login password):

http://www.cisco.com/cgi-bin/Software/Iosplanner/Planner-tool/iosplanner.cgi

This software release is part of a special release of Cisco IOS software that is not released on the same 8-week maintenance cycle that is used for other platforms. As maintenance releases and future software releases become available, they will be posted to Cisco.com in the Cisco IOS software area.

Cisco IOS Release 12.2(25)SEG and later are based on Cisco IOS Release 12.2(25)S. Open caveats in Cisco IOS Release 12.2(25)S also affect Cisco IOS Release 12.2(25)SEG, unless they are listed in the Cisco IOS Release 12.2(25)SEG resolved caveats list. The list of open caveats in Cisco IOS Release 12.2(25)S is available at this URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/prod_release_note09186a00801deec5.html#wp2367913

CISCO SYSTEMS

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Contents

This information is in the release notes:

Hardware Supported

Table 1 lists the hardware supported on Cisco IOS Release 12.2(25)SEG1.

Table 1 Supported Hardware

Device	Description	Supported by Minimum Cisco IOS Release
ME-3400-24TS-A	24 10/100 ports and 2 SFP module slots, AC power	Cisco IOS Release 12.2(25)EX
ME-3400-24TS-D	24 10/100 ports and 2 SFP module slots, DC power	Cisco IOS Release 12.2(25)EX
ME-3400G-12CS-A	12 dual-purpose ports and 4 SFP-only module ports, AC power	Cisco IOS Release 12.2(25)SEG1
ME-3400G-12CS-D	12 dual-purpose ports and 4 SFP-only module ports, AC power	Cisco IOS Release 12.2(25)SEG1
SFP modules	1000BASE-T, -BX, -SX, -LX/LH, -ZX 100BASE-BX, FX, -LX Coarse wavelength-division multiplexing (CWDM)	Cisco IOS Release 12.2(25)EX
Cable	Catalyst 3650 SFP interconnect cable	Cisco IOS Release 12.2(25)EX

Note For configuration information for the Cisco ME-3400-12CS switches, see the *Configuration Notes for the Cisco ME 3400G-12CS Ethernet Access Switch* at this URL: http://www.cisco.com/en/US/products/ps6580/products_installation_and_configuration_guides_list.html

Upgrading the Switch Software

These are the procedures for downloading software. Before downloading software, read this section for important information:

Finding the Software Version and Feature Set

The Cisco IOS image is stored as a bin file in a directory that is named with the Cisco IOS release. The image is stored on the system board flash device (flash:).

You can use the **show version** privileged EXEC command to see the software version that is running on your switch. The second line of the display shows the version.

You can also use the **dir** *filesystem***:** privileged EXEC command to see the directory names of other software images that you might have stored in flash memory.

Deciding Which Files to Use

The upgrade procedures in these release notes describe how to perform the upgrade by using a combined tar file. This file contains the Cisco IOS image file. To upgrade the switch through the command-line interface (CLI), use the tar file and the **archive download-sw** privileged EXEC command.

Table 2 lists the filenames for this software release.

Table 2 Cisco IOS Software Image Files

Filename	Description
me340x-metrobase-tar.122-25.SEG3.tar	Cisco ME 3400 metro base image. This image has basic Metro Ethernet features.
me340x-metrobasek9-tar.122-25.SEG3.tar	Cisco ME 3400 metro base cryptographic image. This image has the Kerberos, Secure Shell (SSH), and basic Metro Ethernet features.
me340x-metroaccess-tar.122-25.SEG3.tar	Cisco ME 3400 metro access image. This image has Layer 2 + Metro Ethernet features.
me340x-metroaccessk9-tar.122-25.SEG3.tar	Cisco ME 3400 metro access cryptographic image. This image has the Kerberos, SSH, and Layer 2 + Metro Ethernet features.

Table 2 Cisco IOS Software Image Files (continued)

Filename	Description
me340x-metroipaccess-tar.122-25.SEG3.tar	Cisco ME 3400 metro IP access image. This image has Layer 2+ and full Layer 3 routing Metro Ethernet features.
me340x-metroipaccess9-tar.122-25.SEG3.tar	Cisco ME 3400 metro IP access cryptographic image. This image has the Kerberos, SSH, Layer 2+, and full Layer 3 routing Metro Ethernet features.

Archiving Software Images

Before upgrading your switch software, make sure that you have archived copies of the current Cisco IOS release and the Cisco IOS release to which you are upgrading. You should keep these archived images until you have upgraded all devices in the network to the new Cisco IOS image and until you have verified that the new Cisco IOS image works properly in your network.

Cisco routinely removes old Cisco IOS versions from Cisco.com. See *Product Bulletin 2863* for more information:

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5187/prod_bulletin0900aecd80281c0e.html

You can copy the bin software image file on the flash memory to the appropriate TFTP directory on a host by using the **copy flash: tftp:** privileged EXEC command.

You can also configure the switch as a TFTP server to copy files from one switch to another without using an external TFTP server by using the **tftp-server** global configuration command. For more information about the **tftp-server** command, see the "Basic File Transfer Services Commands" section of the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2* at this URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a00800ca744.html#wp1018426

Upgrading a Switch

This procedure is for copying the combined tar file to the switch. You copy the file to the switch from a TFTP server and extract the files. You can download an image file and replace or keep the current image.

Note For downloading software, we recommend that you connect to the TFTP server through a network node interface (NNI). If you want to connect to the server through a user network interface (UNI), see the "Troubleshooting" chapter of the software configuration guide for methods for enabling ping capability on UNIs. See the "New Software Features" section on page 6 for a definition of NNIs and UNIs.

To download software, follow these steps:

Step 1 Use Table 2 on page 3 to identify the file that you want to download.

Step 2 Download the software image file. If you have a SmartNet support contract, log in to cisco.com and go to this URL, and log in to download the appropriate files:

http://www.cisco.com/cgi-bin/Software/Iosplanner/Planner-tool/iosplanner.cgi

Click on "*Launch the IOS Upgrade Planner*" and search for ME 3400 to download the appropriate files:

- To download the metro base, metro access, or metro IP access files for a Cisco ME 3400 switch, click **Cisco ME 3400 software**.
- To obtain authorization and to download the cryptographic software files, click **Cisco ME 3400 3DES Cryptographic Software**.

Step 3 Copy the image to the appropriate TFTP directory on the workstation, and make sure that the TFTP server is properly configured.

For more information, refer to Appendix B in the software configuration guide for this release.

Step 4 Log into the switch through the console port or a Telnet session.

Step 5 (Optional) Ensure that you have IP connectivity to the TFTP server by entering this privileged EXEC command:

```
Switch# ping tftp-server-address
```

Note By default, ping is supported on network node interfaces (NNIs), but you cannot ping from a user network interface (UNI) because the control-plane security feature drops ICMP response packets received on UNIs. See the "Troubleshooting" chapter of the software configuration guide for methods for pinging from the switch to a host connected to a UNI.

For more information about assigning an IP address and default gateway to the switch, refer to the software configuration guide for this release.

Step 6 Download the image file from the TFTP server to the switch. If you are installing the same version of software that is currently on the switch, overwrite the current image by entering this privileged EXEC command:

```
Switch# archive download-sw /overwrite /reload
tftp:[[//location]/directory]/image-name.tar
```

The **/overwrite** option overwrites the software image in flash memory with the downloaded one.

The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not saved.

For **//***location*, specify the IP address of the TFTP server.

For **/***directory***/***image-name***.tar**, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

This example shows how to download an image from a TFTP server at 198.30.20.19 and to overwrite the image on the switch:

```
Switch# archive download-sw /overwrite
tftp://198.30.20.19/me340x-metroipaccess-tar.122.25.SEG3.tar
```

You can also download the image file from the TFTP server to the switch and keep the current image by replacing the **/overwrite** option with the **/leave-old-sw** option.

Recovering from a Software Failure

For recovery procedures, see the "Troubleshooting" chapter in the software configuration guide for this release.

Installation Notes

You can assign IP information to your switch by using these methods:

- The CLI-based setup program, as described in the switch hardware installation guide.
- The DHCP-based autoconfiguration, as described in the switch software configuration guide.
- Manually assigning an IP address, as described in the switch software configuration guide.

New Features

These sections describe the new supported hardware and the new software features provided in this release:

- "New Hardware Features" section on page 6
- "New Software Features" section on page 6

New Hardware Features

For a list of all supported hardware, see the "Hardware Supported" section on page 2.

Cisco IOS Release 12.2(25)SEG does not support the Cisco ME-3400G-12CS switches; you must use Cisco IOS Release 12.2(25)SEG1 or later.

Note When you select an IOS product code in the Cisco ordering tool, the selection lists only the 12.2(25)SEG image. However, the image installed on the switch will be the latest available version of the release, in this case 12.2(25)SEG1.

New Software Features

These are new software features for these releases:

- New Software Features for Release 12.2(25)SEG1, page 7
- New Software Features for Release 12.2(25)SEG, page 7

New Software Features for Release 12.2(25)SEG1

These are the new software features for this release:

- Output for the **show policer** and **show platform policer** commands have changed. See the "Control-Plane Security Display Changes" section on page 22.
- Enhanced support for Unique Device Identifier (UDI) feature. See the "Unique Device Identifier (UDI) Enhancement" section on page 20.
- Optional configuration logger to log configuration changes made through the command-line interface (CLI), including the command that was used and who entered it. See the "Configuration Change Logger" section on page 21
- Trunk ports that belong to the same community VLAN can now switch traffic.

  In a UNI community VLAN, local switching is allowed among the ports in the VLAN, but in previous releases, trunk ports belonging to the same community VLAN could not switch traffic.

  Beginning with this release, trunk ports that belong to the same community VLAN can switch all unicast, broadcast, and unknown Layer 2 multicast traffic to other UNI trunk ports in the same community VLAN. However, UNI trunk ports in the same community VLAN cannot switch these traffic types to other UNI trunk ports:

  - Layer 2 IP multicast traffic such as IGMP
  - Applications or protocols that use Layer 2 IP multicast control packets
  - Control protocols that use Layer 3 multicast traffic

  There are no restrictions on traffic between UNI trunk ports and NNI trunk ports, or between a UNI access port and a UNI trunk port that are in the same community VLAN.
- These new software features for the Cisco ME-3400G-12CS switch:
  - Support for the **media-type** interface configuration command to select the active interface for a dual purpose port as either a 10/100/1000 port (using an RJ-45 connector) or an SFP module port.
  - Support for the **power-supply dual** global configuration command to suppress the power-supply alarm when the switch is using a single power supply.
  - Changes in output for the **show env** privileged EXEC command to reflect dual power supplies, dual fans, and increased control of temperature alarm indicators.

  For more information about configuring the Cisco ME-3400G-12CS switch, see the *Configuration Notes for the Cisco ME-3400G-12CS Ethernet Access Switch* at this URL:

  http://www.cisco.com/en/US/products/ps6580/products_installation_and_configuration_guides_list.html

New Software Features for Release 12.2(25)SEG

These are the new software features for this release:

- Support for metro Ethernet operation, administration, and maintenance (OAM) IEEE 802.1ag Connectivity Fault Management (CFM) and Ethernet Local Management Interface (E-LMI). Requires the metro IP access or metro access image.
- Per-port per-VLAN quality of service (QoS) using hierarchical policy maps. Requires the metro IP access or metro access image.

- Support for all Open Shortest Path First (OSPF) network types—broadcast, nonbroadcast multiaccess (NBMA), point-to-point, or point-to-multipoint networks. Requires the metro IP access image.
- Nonstop forwarding (NSF) awareness enables the Layer 3 switch to continue forwarding packets from an NSF-capable neighboring router when the primary route processor (RP) is failing and the backup RP is taking over or while the primary RP is manually reloaded for a nondisruptive software upgrade. Requires the metro IP access image.
- Support for Intermediate System-to-Intermediate System (IS-IS) dynamic routing protocols for ISO CLNS networks. Requires the metro IP access image.
- NNI port-type configuration allowed on all ports. Requires the metro IP access image.
- Link-state tracking mirrors the state of ports carrying upstream traffic from connected hosts and servers. The server traffic can then failover to an operational link on another Cisco Ethernet switch. Requires the metro IP access or metro access image.
- Flex Link preemptive switchovers so that you can configure a Flex Link to complete a master switchover, and Flex Link sub-100 ms convergence. Requires the metro IP access or metro access image.
- Layer 2 protocol tunneling on trunk ports. Requires the metro IP access or metro access image.
- DHCP server capability.
- Multiple spanning-tree (MST) based on the IEEE 802.1s standard.
- Support for CNS image agent for downloading a new image to a switch.
- Option-82 enhancement that allows users to configure the remote-ID and circuit-ID suboptions.
- Secure Copy Protocol (SCP) provides a secure and authenticated method for copying switch configuration or switch image files. Requires the cryptographic version of the software.
- Support for the CISCO-DHCP-SNOOPING-MIB that provides SNMP management support for DHCP snooping.

Minimum Cisco IOS Release for Major Features

Table 3 lists the minimum software release (after the first release) required to support the major features of the Cisco ME 3400 switch. Features not listed are supported in all releases.

Table 3 Features Introduced After the First Release and the Minimum Cisco IOS Release Required

Feature	Minimum Cisco IOS Release Required
Ethernet OAM 802.1ag and E-LMI (metro IP access and metro access images only)	12.2(25)SEG
Per port per VLAN QoS (metro IP access and metro access images only)	12.2(25)SEG
Support for all OSPF network types (metro IP access only)	12.2(25)SEG
Layer 2 protocol tunneling on trunks (metro IP access and metro access images only)	12.2(25)SEG
IS-IS protocol (metro IP access only)	12.2(25)SEG
NNIs on all ports (metro IP access image only)	12.2(25)SEG
DHCP server	12.2(25)SEG
DHCP Option-82 configurable remote ID and circuit ID	12.2(25)SEG

Table 3 Features Introduced After the First Release and the Minimum Cisco IOS Release Required (continued)

Feature	Minimum Cisco IOS Release Required
Multiple spanning-tree (MST) based on the IEEE 802.1s standard	12.2(25)SEG
Nonstop forwarding (NSF) awareness (metro IP access image only)	12.2(25)SEG
Secure Copy Protocol	12.2(25)SEG
Flex Links sub 100 ms convergence and preemptive switchover (metro IP access and metro access images only)	12.2(25)SEG
Link-state tracking (trunk failover) (metro IP access and metro access images only)	12.2(25)SEG

Limitations and Restrictions

You should review this section before you begin working with the switch. These are known limitations that will not be fixed, and there is not always a workaround. Some features might not work as documented, and some features could be affected by recent changes to the switch hardware or software.

These limitations apply to the Cisco ME switches:

Configuration

These are the configuration limitations:

- A static IP address might be removed when the previously acquired DHCP IP address lease expires.

  This problem occurs under these conditions:

  - When the switch is booted without a configuration (no config.text file in flash memory).
  - When the switch is connected to a DHCP server that is configured to give an address to it (the dynamic IP address is assigned to VLAN 1).
  - When an IP address is configured on VLAN 1 before the dynamic address lease assigned to VLAN 1 expires.

  The workaround is to reconfigure the static IP address. (CSCea71176 and CSCdz11708)

- The DHCP snooping binding database is not written to flash memory or a remote file in any of these situations:
  - When the Network Time Protocol (NTP) is configured, but the NTP clock is not synchronized. You can check the clock status by entering the **show NTP status** privileged EXEC command and verifying that the network connection to the NTP server and the peer work correctly.
  - The DHCP snooping database file is manually removed from the file system. After enabling the DHCP snooping database by configuring a database URL, a database file is created. If the file is manually removed from the file system, the DHCP snooping database does not create another database file. You need to disable the DHCP snooping database and enable it again to create the database file.
  - The URL for the configured DHCP snooping database was replaced because the original URL was not accessible. The new URL might not take effect after the timeout of the old URL.

  No workaround is necessary; these are the designed behaviors. (CSCed50819)
- When dynamic ARP inspection is enabled on a switch, ARP and RARP packets greater than 2016 bytes are dropped by the switch or switch stack. This is a hardware limitation.

  However, when dynamic ARP inspection is not enabled and a jumbo MTU is configured, ARP and RARP packets are correctly bridged in hardware. (CSCed79734)
- Dynamic ARP inspection log entries might be lost after a switch failure. Any log entries that are still in the log buffer (have not been output as a system message) on a switch that fails are lost.

  When you enter the **show ip arp inspection log** privileged EXEC command, the log entries from all switches in the stack are moved to the switch on which you entered the command.

  There is no workaround. (CSCed95822)
- When port security is enabled on an interface in restricted mode and the **switchport block unicast interface** command has been entered on that interface, MAC addresses are incorrectly forwarded when they should be blocked

  The workaround is to enter the **no switchport block unicast** interface configuration command on that specific interface. (CSCee93822)
- A traceback error occurs if a crypto key is generated after an SSL client session.

  There is no workaround. This is a cosmetic error and does not affect the functionality of the switch. (CSCef59331)

IP

These are the IP limitations:

- Subnetwork Access Protocol (SNAP) encapsulated IP packets are dropped without an error message being reported at the interface. The switch does not support SNAP-encapsulated IP packets. There is no workaround. (CSCdz89142)
- The switch does not create an adjacent table entry when the ARP timeout value is 15 seconds and the ARP request times out. The workaround is to not set an ARP timeout value lower than 120 seconds. (CSCea21674)

MAC Addressing

This is the MAC addressing limitation:

When a MAC address is configured for filtering on the internal VLAN of a routed port, incoming packets from the MAC address to the routed port are not dropped. (CSCeb67937)

Multicasting

These are the multicasting limitations:

- The switch does not support tunnel interfaces, including DVMRP and PIM tunneling.
- Nonreverse-path forwarded (RPF) IP multicast traffic to a group that is bridged in a VLAN is leaked onto a trunk port in the VLAN even if the port is not a member of the group in the VLAN, but it is a member of the group in another VLAN. Because unnecessary traffic is sent on the trunk port, it reduces the bandwidth of the port. There is no workaround for this problem because non-RPF traffic is continuous in certain topologies. As long as the trunk port is a member of the group in at least one VLAN, this problem occurs for the non-RPF traffic. (CSCdu25219)
- If the number of multicast routes and Internet Group Management Protocol (IGMP) groups are more than the maximum number specified by the **show sdm prefer** global configuration command, the traffic received on unknown groups is flooded in the received VLAN even though the **show ip igmp snooping multicast-table** privileged EXEC command output shows otherwise. The workaround is to reduce the number of multicast routes and IGMP snooping groups to less than the maximum supported value. (CSCdy09008)
- IGMP filtering is applied to packets that are forwarded through hardware. It is not applied to packets that are forwarded through software. Hence, with multicast routing enabled, the first few packets are sent from a port even when IGMP filtering is set to deny those groups on that port. There is no workaround. (CSCdy82818)
- When you use the **ip access-group** interface configuration command with a router access control list (ACL) to deny access to a group in a VLAN, multicast data to the group that is received in the VLAN is always flooded in the VLAN, regardless of IGMP group membership in the VLAN. This provides reachability to directly connected clients, if any, in the VLAN. The workaround is to not apply a router ACL set to deny access to a VLAN interface. Apply the security through other means; for example, apply VLAN maps to the VLAN instead of using a router ACL for the group. (CSCdz86110)
- If an IGMP report packet has two multicast group records, the switch removes or adds interfaces depending on the order of the records in the packet:
  - If the ALLOW_NEW_SOURCE record is before the BLOCK_OLD_SOURCE record, the switch removes the port from the group.
  - If the BLOCK_OLD_SOURCE record is before the ALLOW_NEW_SOURCE record, the switch adds the port to the group.

  There is no workaround. (CSCec20128)
- When IGMP snooping is disabled and you enter the **switchport block multicast** interface configuration command, IP multicast traffic is not blocked.

  The **switchport block multicast** interface configuration command is only applicable to non-IP multicast traffic.

  There is no workaround. (CSCee16865)

- Incomplete multicast traffic can be seen under either of these conditions:
  - You disable IP multicast routing or re-enable it globally on an interface.
  - A switch mroute table temporarily runs out of resources and recovers later.

  The workaround is to enter the **clear ip mroute** privileged EXEC command on the interface. (CSCef42436)

Routing

These are the routing limitations:

- The switch does not support tunnel interfaces for routed traffic.
- A route map that has an ACL with a Differentiated Services Code Point (DSCP) clause cannot be applied to a Layer 3 interface. The switch rejects this configuration and displays a message that the route map is unsupported. There is no workaround. (CSCea52915)
- A spanning-tree loop might occur if all of these conditions are true:
  - Port security is enabled with the violation mode set to protected.
  - The maximum number of secure addresses is less than the number of switches connected to the port.
  - There is a physical loop in the network through a switch whose MAC address has not been secured, and its BPDUs cause a secure violation.

  The workaround is to change any one of the listed conditions. (CSCed53633)

QoS

This is a quality of service (QoS) limitation:

- CSCsb98219

  When you use the **bandwidth** policy-map class command to configure more than one class in a policy map for Class-based Weighted Fair Queuing (CBWFQ), and the committed information rate (CIR) bandwidth for any of the classes is less than 2 percent of the interface rate, the CBWFQ classes in the policy may not receive the configured CIR bandwidths.

  There is no workaround, but it is unlikely that a CBWFQ class would be configured with such a low CIR bandwidth.

SPAN and RSPAN

These are the SPAN and Remote SPAN (RSPAN) limitations.

- The egress SPAN data rate might degrade when multicast routing is enabled. The amount of degradation depends on the processor loading. Typically, the switch can egress SPAN at up to 40,000 packets per second (64-byte packets). As long as the total traffic being monitored is below this limit, there is no degradation. However, if the traffic being monitored exceeds the limit, only a portion of the source stream is spanned. When this occurs, the following console message appears: `Decreased egress SPAN rate`. In all cases, normal traffic is not affected; the degradation limits only how much of the original source stream can be egress spanned. If multicast routing is disabled, egress SPAN is not degraded. There is no workaround. If possible, disable multicast routing. If possible, use ingress SPAN to observe the same traffic. (CSCeb01216)

- Some IGMP report and query packets with IP options might not be ingress-spanned. Packets that are susceptible to this problem are IGMP packets containing 4 bytes of IP options (IP header length of 24). An example of such packets would be IGMP reports and queries having the router alert IP option. Ingress-spanning of such packets is not accurate and can vary with the traffic rate. Typically, very few or none of these packets are spanned. There is no workaround. (CSCeb23352)
- Cisco Discovery Protocol (CDP) and Port Aggregation Protocol (PAgP) packets received by network node interfaces (NNIs) from a SPAN source are not sent to the destination interfaces of a local SPAN session. The workaround is to use the **monitor session** *session_number* **destination** {**interface** *interface-id* **encapsulation replicate**} global configuration command for local SPAN. (CSCed24036)

Trunking

These are the trunking limitations:

- IP traffic with IP options set is sometimes leaked on a trunk port. For example, a trunk port is a member of an IP multicast group in VLAN X but is not a member in VLAN Y. If VLAN Y is the output interface for the multicast route entry assigned to the multicast group and an interface in VLAN Y belongs to the same multicast group, the IP-option traffic received on an input VLAN interface other than one in VLAN Y is sent on the trunk port in VLAN Y because the trunk port is forwarding in VLAN Y, even though the port has no group membership in VLAN Y. There is no workaround. (CSCdz42909).
- For trunk ports or access ports configured with IEEE 802.1Q tagging, inconsistent statistics might appear in the **show interfaces counters** privileged EXEC command output. Valid IEEE 802.1Q frames of 64 to 66 bytes are correctly forwarded even though the port LED blinks amber, and the frames are not counted on the interface statistics. There is no workaround. (CSCec35100).

VLAN

These are the VLAN limitations:

- If the number of VLANs times the number of trunk ports exceeds the recommended limit of 13,000, the switch can fail.

  The workaround is to not configure more than the recommended number of VLANs and trunks. (CSCeb31087)
- A CPUHOG message sometimes appears when you configure a private VLAN. Enable port security on one or more of the ports affected by the private VLAN configuration.

  There is no workaround. (CSCed71422)

Open Caveats

This section describes the open caveats in this software release.

- CSCeh54035

  When IGMP snooping is disabled on the switch, CPU control-plane security does not prevent IGMP packets received on UNI ports from being sent to the CPU.

  The workaround is to not disable IGMP snooping if you want CPU control-plane security to be in effect for IGMP packets.

- CSCsb84285

  Although the configuration is not supported, the ME 3400 switch allows you to enter the **ip vrf forwarding** *vrf-name* interface configuration command (to associate a VPN routing and forwarding table with a Layer 3 interface) on private VLAN interfaces.

  The workaround is to not configure VRF on private VLAN interfaces

- CSCsc20515

  If you create a private VLAN domain with a primary and secondary VLAN, configure the secondary VLAN as a community VLAN, and then use the **switchport private-vlan host** and **switchport private-vlan host-association** interface configuration commands to associate ports to the private VLAN, the LEDs on the ports that belong to the secondary VLAN display as amber. However, if you then use the **monitor session** *session_number* **destination interface** *interface-id* global configuration command for one of these ports to configure it as a SPAN destination port and later configure it again as a member of the secondary community VLAN, the LED changes to green.

  The workaround is to use the **shutdown** and then **no shutdown** interface configuration commands on the interface. The change of state from down to up results in the interface correctly showing as amber.

- CSCsc21602

  You cannot attach an output policy-map that has a class associated with qualified queue-limit to an interface when all queue-limit qualifiers are correctly represented by the associated class-map classification criteria, but the class map has one or more classification criteria that are not represented by any queue-limit qualifiers. This error message appears even when the condition mentioned in the message is satisfied:

  ```
  QoS: Configuration failed. All queue-limit qualifier criteria must be represented
  within the associated class-map classification criteria
  ```

Note A *qualified queue limit* is when you configure a different queue limit for one or more different classification criteria of the class map, for example by entering the command **queue-limit dscp 30 48**.

  The same error message appears when a policy map with a qualified queue-limit is attached to an interface and a class-map classification criteria not associated with any configured queue-limit qualifier is added to the class map associated with qualified queue-limit. In this case, in spite of the error message, the configuration is accepted.

  The same error message also appears when a policy-map with qualified queue-limit is attached to an interface and a class-map classification criteria already associated with a configured queue-limit qualifier is deleted from the class map associated with qualified queue-limit. In this case also, in spite of the error message, the configuration is accepted.

The workaround is when you configure an output policy-map with qualified queue-limit, you should ensure that each classification criteria in the class-map associated with qualified queue-limit is represented by a unique qualified queue-limit. The threshold value to which each queue-limit qualifier is mapped is flexible and based on requirements.

In the cases in which the configuration is accepted even after the error message is displayed, you can ignore the error message.

- CSCsc26465

  When a CWDM-type SFP module is installed in the switch, the CWDM device is not listed in the output of the **show inventory** User EXEC command.

  The workaround is to use the **show inventory raw** User EXEC command. to see a listing of all entities in the switch.

- CSCse21219

  If a Putty client is used to change the configuration to a device with SSH, the switch might stop responding to incoming traffic, such as SSH, Telnet, or ping packets. The switch responds to traffic after the TCP session is reset, which can take 7 minutes.

  Use one of these workarounds:

  - Use Putty Version 0.58.
  - Enter a SSH, telnet, or ping command on the console.

- CSCse07183

  When you enter the **service-policy input** *parent-policy- map-name* interface configuration command to attach a per-port per-VLAN service policy, if two or more classes in the per-port per-VLAN parent policy contain the same VLAN, the attachment fails and this error message appears:

  ```
  QoS: hqm_qoscli_classmap_filter_update_in_servpolicy Overlapping vlan is not allowed
  in class and class
  ```

  This is because classes with overlapping VLANs are not allowed within a per-port per-VLAN parent policy. Overlapping VLAN classes occur when two or more class-maps in a per-port per-VLAN parent policy contain match statements the specify the same VLAN.

  The workaround is to consolidate overlapping per-port per-VLAN parent classes with overlapping VLANs and to configure per-port per-VLAN child policy classes to classify and act on traffic as desired.

- CSCse11323

  When 256 policy maps are configured globally on the system, the creation of the 257th policy map is rejected. The platform supports a maximum of 256 policy maps. If you then delete some existing policy maps and again configure the rejected policy map, when you try to attach that policy map to an interface, it might be rejected without any descriptive error message explaining the reason for the rejection or with an unexpected and incorrect error message.

  The workaround is to delete the problematic policy map and to reconfigure it with a different name. The new policy map should be accepted as expected.

- CSCse36402

  When a per-port per-VLAN QoS policy is attached to multiple trunk interfaces and one of the interfaces is changed to a routed port, the policy is detached from all interfaces.

  The workaround is to use the **service-policy input** *parent-policy- map-name* interface configuration command to reattach the detached per-port per-VLAN parent policies to the trunk interfaces. Traffic then receives the correct QoS treatment.

- CSCse38455

  When more than 47 unique policers are configured in a per-port or a per-port per-VLAN hierarchical input policy map that is attached to an interface, unexpected and incorrect QoS behavior might occur for traffic that matches classes assigned to policers after the first 47. The control-plane security on UNI ports might also be compromised.

  The workaround is to not configure more than 47 policers on a port, even if the configuration is accepted. The switch supports a maximum of 47 unique policers per port.

Resolved Caveats

These are the caveats that have been resolved in these releases:

- Caveats Resolved in Cisco IOS Release 12.2(25)SEG3, page 16
- Caveats Resolved in Cisco IOS Release 12.2(25)SEG1, page 17
- Caveats Resolved in Cisco IOS Release 12.2(25)SEG, page 18

Caveats Resolved in Cisco IOS Release 12.2(25)SEG3

These are the resolved caveats in Cisco IOS Release 12.2(25)SEG3:

- CSCsd95616

  Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS software that may lead to a denial of service (DoS) condition. Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-multicast.shtml.

- CSCsf04754

  Multiple Cisco products contain either of two authentication vulnerabilities in the Simple Network Management Protocol version 3 (SNMPv3) feature. These vulnerabilities can be exploited when processing a malformed SNMPv3 message. These vulnerabilities could allow the disclosure of network information or may enable an attacker to perform configuration changes to vulnerable devices. The SNMP server is an optional service that is disabled by default. Only SNMPv3 is impacted by these vulnerabilities. Workarounds are available for mitigating the impact of the vulnerabilities described in this document.

  The United States Computer Emergency Response Team (US-CERT) has assigned Vulnerability Note VU#878044 to these vulnerabilities.

  Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-0960 has been assigned to these vulnerabilities.

  This advisory will be posted at http://www.cisco.com/warp/public/707/cisco-sa-20080610-snmpv3.shtml

- CSCsj44081

  Improvements have been made to User Datagram Protocol (UDP) processing.

Caveats Resolved in Cisco IOS Release 12.2(25)SEG1

These are the resolved caveats in Cisco IOS Release 12.2(25)SEG1:

- CSCef73145

  The Mean Opinion Score (MOS) reported by an IP SLA jitter probe is now correct.

- CSCsb81283

  MAC notifications now work properly when port security is configured.

- CSCsd26663

  The switch no longer drops ICMPv6 router advertisements that are encapsulated in Ethernet frames with unicast or unknown destination addresses.

- CSCsd51530

  When you telnet to a switch and enter the **autocommand-options nohangup** interface configuration command on VTY lines 0 through 4, you can now successfully log out and telnet back into the switch.

  In previous releases, when you logged out of the switch and then tried to open a new Telnet session, the switch would automatically log you out.

- CSCse17494

  When a switch is running Cisco Network Assistant and using TACACS+ for HTTPS (secure HTTP) authentication, the switch no longer fails if TACACS+ is not reachable.

- CSCse29173

  Layer 2 multicast traffic is now forwarded by a switch after a port-channel link flap.

- CSCse39616

  When port security is enabled, MAC addresses are now correctly relearned if a dynamic instance is present on the remote port.

- CSCse47012

  When a hierarchical port-shaping output policy-map with child class-based actions is attached to an interface, and an input policy map attached to any interface is modified or removed and then re-attached, the class-based actions in the hierarchical output policy-map now continue to operate.

- CSCse50641

  If you try to attach an output policy map with a qualified queue-limit value based on a QoS group to an interface, and the QoS group number is greater than 15, the policy-map attachment no longer fails, and no error message appears.

- CSCse59236

  If a Gigabit Ethernet interface is connected to a Fast Ethernet link and an output policy map with a shaping action is attached to the interface, when the configuration is saved and the system reloads, the output policy is now correctly attached to the interface after the reload with no error message.

Caveats Resolved in Cisco IOS Release 12.2(25)SEG

These are the resolved caveats in Cisco IOS Release 12.2(25)SEG:

- CSCeh16869

  In an multiple spanning-tree (MST) region in which Switch 1 is connected to Switch 2 and Switch 2 is connected to Switch 3, if Switch 2 has a root port and a designated port in MST instance 2, the port that you configure as the designated MST port now synchronizes.

- CSCeh19672

  If an IEEE 802.1x client configured for both machine and user authentication is connected to a switch and RADIUS VLAN assignment is used only for the machine authentication, the user authentication no longer takes 2 to 5 minutes.

- CSCek26492

  Symptoms: A router may crash if it receives a packet with a specific crafted IP option as detailed in Cisco Security Advisory: Crafted IP Option Vulnerability:

  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

  Conditions: This DDTS resolves a symptom of CSCec71950. Cisco IOS with this specific DDTS are not at risk of crash if CSCec71950 has been resolved in the software.

  Workaround: Cisco IOS versions with the fix for CSCec71950 are not at risk for this issue and no workaround is required. If CSCec71950 is not resolved, see the following Cisco Security Advisory: Crafted IP Option Vulnerability for workaround information:

  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

- CSCek37177

  The Cisco IOS Transmission Control Protocol (TCP) listener in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable memory leak that may lead to a denial of service condition.

  This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability.

  Cisco has made free software available to address this vulnerability for affected customers.

  This issue is documented as Cisco bug ID CSCek37177.

  There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml

- CSCsc14748

  When a port belongs to a private VLAN primary VLAN and also belongs to VLAN 1, deleting the primary VLAN no longer might shut down the line protocol for the port's switch virtual interface (SVI) on VLAN 1.

- CSCsc16012

  When you use the **bandwidth percent** policy-map class command to configure a class in a policy map, attach the policy map to an interface, and configure the same policy map as a child policy to a parent port-shaping policy map that is also attached to an interface, the **show policy-map interface** *interface-id* user EXEC command for the latter interface now shows the correct bandwidth for the class configured with the **bandwidth percent** command.

- CSCsc17257

  When you configure an input policy map that uses a table map to map an incoming CoS (IEEE 801.1p bit) value (*from* cos) to another packet marking, the switch no longer allows you to attach the policy map to a port that cannot receive IEEE 802.1Q or IEEE 802.1p tagged packets.

- CSCsb69676

  When individual policing or aggregate policing is configured in a policy map with the policing exceed-action based on table maps, after the policy is attached to an interface you can now overwrite the configuration with a new police exceed-action based an a different table map.

- CSCsb86336

  When you enter the **bandwidth remaining percent** *value* policy-map class configuration command or the **bandwidth percent** *value* policy-map class configuration command, you no longer receive an incorrect error message.

- CSCsc24495

  When an output hierarchical port-shaping policy map with a child policy that has CoS classification is attached to a trunk interface and the interface is later changed to a nontrunk interface, the policy map is now correctly detached.

- CSCsb74925

  When you are configuring a large number of ports as SPAN destination ports, you no longer receive a traceback message.

- CSCsc30193

  When you configure an input policy-map with a **set** action that references an invalid table map, the configuration is correctly rejected with an error message, and packets no longer might be incorrectly marked for that class. (A table map is invalid for a **set** action when the value of the *from-* or *to-* type parameter of the table map is inconsistent with the *from-* or *to-* type specified in the **set** action.)

- CSCsc30194

  When one output policy map (*policy-map1*) that is attached to an interface has a class configured for an unqualified queue-limit or no queue-limit at all, and another output policy map (*policy-map2*) attached to the interface has a qualified queue limit configured for the same class, detaching *policy-map1* from the interface before you detach *policy-map2* no longer might cause an incorrect queue limit to be applied to some packets in the class.

Note An *unqualified queue limit* is a single queue limit that applies to all the classification criteria of the class map, configured by entering the **queue-limit** *number-of-packets* policy-map class command.
A *qualified queue limit* is the configuration of a different queue limit for one or more different classification criteria of the class map, for example by entering the command **queue-limit dscp 30 48**.

- CSCsc30211

  When an output policy map (*policy-map1*) that has a class configured for an unqualified queue-limit is *attached* to an interface before another output policy map (*policy-map2*) that has a qualified queue limit configured for the same class is attached to an interface, the queue limit applied for all packets matching the specified class for *policy map1* is the user-configured unqualified queue-limit value.

Note An *unqualified queue limit* is a single queue limit that applies to all the classification criteria of the class map, configured by entering the **queue-limit** *number-of-packets* policy-map class command.
A *qualified queue limit* is the configuration of a different queue limit for one or more different classification criteria of the class map, for example by entering the command **queue-limit dscp 30 48**.

- CSCsc35915

  The documentation now correctly states that you can configure no more than 47 policers per port and 228 policers per switch. One policer is reserved for internal use.

Documentation Updates

This section contains documentation updates.

Documentation Updates for Cisco IOS Release 12.2(25)SEG1

These are the updates to documentation for this release.

For more information about the Cisco ME-3400G-12CS switch, see these documents:

- *Configuration Notes for the Cisco ME-3400G-12CS Ethernet Access Switch* at this URL:

  http://www.cisco.com/en/US/products/ps6580/products_installation_and_configuration_guides_list.html

- *Cisco ME 3400 Ethernet Access Switch Hardware Installation Guide, September, 2006* at this URL:

  http://www.cisco.com/en/US/products/ps6580/prod_installation_guides_list.html

Unique Device Identifier (UDI) Enhancement

The **show inventory** [**raw**] user EXEC command allows you to display product identification (PID) information for all identifiable entities in the device. Beginning with this release, you can use the **show inventory** *entity-name* command to display a specific entity. For example, if you enter **show inventory gigabitethernet 0/1**, the output displays the identity of the small form-factor pluggable (SFP) module installed in SFP module port gigabitethernet 0/1. The display shows the UDI, including PID, Version Identifier (VID), and Serial Number (SN) of that entity.

Note If you enter **show inventory ?** in the CLI help, the *entity-name* keyword does not appear in this release of the software, although it is supported, and you can enter an entity name.

Configuration Change Logger

Beginning with this release, you can enable a configuration logger to keep track of configuration changes made with the CLI. When you enter the **logging enable** configuration-change logger configuration command, the log records the session, the user, and the command that was entered to change the configuration. You can configure the size of the configuration log from 1 to 1000 entries (the default is 100). You can clear the log at any time by entering the **no logging enable** command followed by the **logging enable** command to disable and reenable logging.

Use the **show archive log config** {**all** | *number* [*end-number*] | **user** *username* [**session** *number*] *number* [*end-number*] | **statistics**} [**provisioning**] privileged EXEC command to display the complete configuration log or the log for specified parameters.

The default is that configuration logging is disabled.

For information about the commands, see the *Cisco IOS Configuration Fundamentals and Network Management Command Reference, Release 12.3 T* at this URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_command_reference_chapter09186a00801a8086.html#wp1114989

Beginning in privileged EXEC mode, follow these steps to enable configuration logging:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**archive**	Enter archive configuration mode.
Step 3	**log config**	Enter configuration-change logger configuration mode.
Step 4	**logging enable**	Enable configuration change logging.
Step 5	**logging size** *entries*	(Optional) Configure the number of entries retained in the configuration log. The range is from 1 to 1000. The default is 100. **Note** When the configuration log is full, the oldest log entry is removed each time a new entry is entered.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show archive log config**	Verify your entries by viewing the configuration log.

This example shows how to enable the configuration-change logger and to set the number of entries in the log to 500.

```
Switch(config)# archive
Switch(config-archive)# log config
Switch(config-archive-log-cfg)# logging enable
Switch(config-archive-log-cfg)# logging size 500
Switch(config-archive-log-cfg)# end
```

This is an example of output for the configuration log:

```
Switch# show archive log config all
 idx   sess           user@line      Logged command
   38    11   unknown user@vty3     |no aaa authorization config-commands
   39    12   unknown user@vty3     |no aaa authorization network default group radius
   40    12   unknown user@vty3     |no aaa accounting dot1x default start-stop group
radius
   41    13   unknown user@vty3     |no aaa accounting system default
   42    14           temi@vty4     |interface GigabitEthernet4/0/1
   43    14           temi@vty4     | switchport mode trunk
   44    14           temi@vty4     | exit
   45    16           temi@vty5     |interface FastEthernet5/0/1
   46    16           temi@vty5     | switchport mode trunk
   47    16           temi@vty5     | exit
```

Control-Plane Security Display Changes

Output display formats have changed for the **show policer cpu uni drop** and **show policer cpu uni drop interface** user EXEC commands, and for the **show platform policer cpu interface** privileged EXEC command.

In the **show policer cpu uni drop** output, the Port Name field replaces the Policer Num field. This is an example of the output for this command:

```
Switch# show policer cpu uni drop
================================
Port                 In           Dropped
Name               Frames          Frames
========================================
Port                 In           Dropped
Name               Frames          Frames
Fa0/1                300              0
Fa0/2                  0              0
Fa0/3                  0              0
Fa0/4                  0              0
Fa0/5                200              0
Fa0/6                  0              0
Fa0/7                  0              0
Fa0/8                  0              0
Fa0/9             508055         325086
Fa0/10                 0              0
Fa0/11                 0              0
Fa0/12                 0              0
Fa0/13                 0              0
Fa0/14                 0              0
Fa0/15                 0              0
Fa0/16                 0              0
Fa0/17                 0              0
Fa0/18                 0              0
Fa0/19                 0              0
Fa0/20                 0              0
Fa0/21                 0              0
Fa0/22                 0              0
Fa0/23                 0              0
Fa0/24                 0              0
Gi0/1                  0              0
Gi0/2                  0              0
drop-all               0        1849645
```

This is an example of the new output format for the **show policer cpu uni drop interface** command:

```
Switch# show policer cpu uni drop interface gigabitethernet 0/1
============================
Policer assigned for Gi0/2
============================
Protocols using this policer:
"VTP" "CISCO_L2" "KEEPALIVE" "SWITCH_IGMP" "SWITCH_L2PT"
Policer rate: 160000 bps
In frames: 48014
Drop frames: 28630
```

The **show platform policer cpu interface** output now includes a column displaying the ASIC number to make it clear when policers are on different ASICs. These are examples of outputs for this command:

```
Switch# show platform policer cpu interface fastethernet 0/3
Policers assigned for CPU protection
=====================================================================
 Feature                          Policer        Physical      Asic
                                  Index          Policer       Num
=====================================================================
Fa0/3
STP                                  1            26             0
LACP                                 2            26             0
8021X                                3            26             0
RSVD_STP                             4            26             0
PVST_PLUS                            5            26             0
CDP                                  6            26             0
DTP                                  7            26             0
UDLD                                 8            26             0
PAGP                                 9            26             0
VTP                                 10            26             0
CISCO_L2                            11            26             0
KEEPALIVE                           12             2             0
CFM                                 13           255             0
SWITCH_MAC                          14            26             0
SWITCH_ROUTER_MAC                   15            26             0
SWITCH_IGMP                         16             2             0
SWITCH_L2PT                         17             2             0

Switch# show platform policer cpu interface fastethernet 0/5
Policers assigned for CPU protection
=====================================================================
 Feature                          Policer        Physical      Asic
                                  Index          Policer       Num
=====================================================================
Fa0/5
STP                                  1            26             1
LACP                                 2            26             1
8021X                                3            26             1
RSVD_STP                             4            26             1
PVST_PLUS                            5            26             1
CDP                                  6            26             1
DTP                                  7            26             1
UDLD                                 8            26             1
PAGP                                 9            26             1
VTP                                 10            26             1
CISCO_L2                            11            26             1
KEEPALIVE                           12             2             1
CFM                                 13           255             1
SWITCH_MAC                          14            26             1
SWITCH_ROUTER_MAC                   15            26             1
SWITCH_IGMP                         16             2             1
SWITCH_L2PT                         17             2             1
```

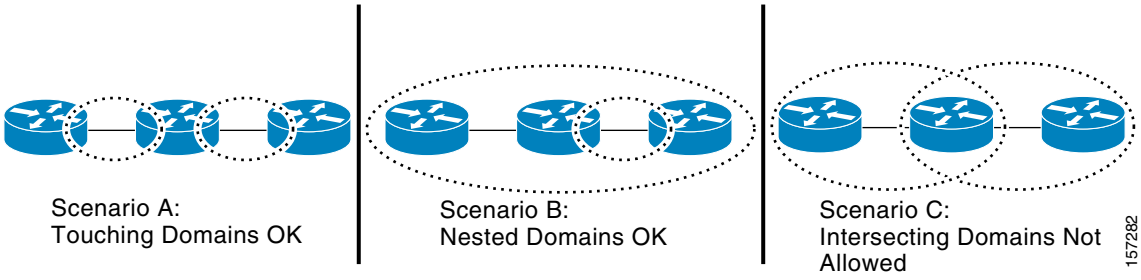
Documentation Updates for Cisco IOS Release 12.2(25)SEG

This section includes the updates to documentation for this release.

Correction to the Software Configuration Guide

In Chapter 34, "Configuring Ethernet CFM and E-LMI," Figure 34-2 originally showed incorrect examples for Scenario B and Scenario C. The illustration has been corrected as shown below:

Figure 34-2 Allowed Domain Relationships



IP SLAs Support

The Cisco ME 3400 switch includes partial support for Cisco IOS IP Service Level Agreements (IP SLAs) to provide advanced network service monitoring information and collect data pertaining to SLAs verification. The switch can initiate and reply jitter probes. However, the traffic does not follow the queuing configuration that is applied to customer traffic. All locally originated traffic always goes to the same egress queue on the switch port, regardless of the ToS setting for the IP SLAs probe. We recommend the use of an external shadow router to measure latency and packet drop rate (PDR) across the switch.

For performance testing purposes, this configuration was validated:

1. Two switches connected back-to-back.
2. No protocols running on the switch CPUs, including STP.
3. Jitter probe send and receive rate:
   a. 50 bidirectional probes sent with each probe consisting of up to 50 packets sent at 1-second intervals.
   b. Probes started with a 1-second stagger between each probe.

For information about IP SLAs on Cisco routers, see this URL:

http://www.cisco.com/application/pdf/en/us/guest/products/ps6602/c1244/cdccont_0900aecd804fb392.pdf

Correction to the Getting Started Guide

In Step 5 of the "Initial Setup" section, the maximum power consumption is listed as 40 W. The correct maximum power consumption is 30 W.

Correction to the RCSI

This warning will be added to the *Regulatory Compliance and Safety Information (RCSI):*

Warning **Suitable for mounting on and over a concrete or other non-combustible surface only.** Statement 345

Waarschuwing **Kan alleen worden bevestigd op of boven een betonnen of andere niet-ontvlambare ondergrond.**

Varoitus **Sopii kiinnitettäväksi vain betonipintaan tai muuhun palamattomaan pintaan tai niiden yläpuolelle.**

Attention **Adapté uniquement pour un montage au mur ou sur une surface en béton ou autre surface incombustible.**

Warnung **Nur geeignet zum Anbringen an oder auf Beton- oder anderen feuerfesten Oberflächen.**

Avvertenza **Da applicare o montare esclusivamente su cemento o altre superfici non combustibili.**

Advarsel **Bare for montering på eller over betongoverflater eller andre ikke-brennbare overflater.**

Aviso **Adequado apenas para montagem em ou sobre concreto ou outra superfície não combustível.**

¡Advertencia! **Adecuado sólo para su instalación en o sobre cemento u otra superficie no inflamable.**

Varning! **Passar endast för montering på eller ovanför cementyta eller annan ej antändlig yta.**

Csak beton, vagy más nem gyúlékony, felületen/felületre szabad elhelyezni.

Предупреждение Годится для установки только на бетонной или другой негорючей вертикальной или горизонтальной поверхности.

警告 仅适合安装在混凝土表面或其他非易燃表面上。

警告 コンクリートまたはその他の不燃性の表面（垂直か水平）に取り付けてください。

Update to the Hardware Installation Guide

This information is being added to the "Wiring the DC-Input Power Source" section of Appendix C, "Connecting to DC Power," in the *Cisco ME 3400 Ethernet Access Switch Hardware Installation Guide*:

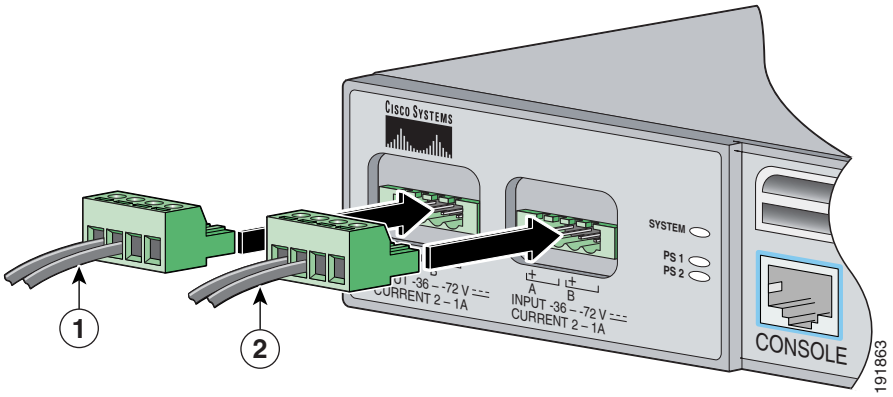
Before you wire the DC-input power source, review the warnings in this section and this information:

If the switch software detects that the circuit boards are not receiving power from an internal power supply, the software sends a message like this to the console:

```
00:06:54: %POWER_SUPPLIES-3-PWR_FAIL: Power supply 2 is not functioning
00:06:54: %PLATFORM_ENV-1-DUAL_PWR: Faulty internal power supply 2 detected
```

This message means that an internal power supply is not providing power. To receive this alert if power fails on the ME 3400G-12CS-DC switch with two power feeds, we recommend that you connect one feed to the left DC power terminal block and the other to the right DC power terminal block. (See the example in Figure 1.)

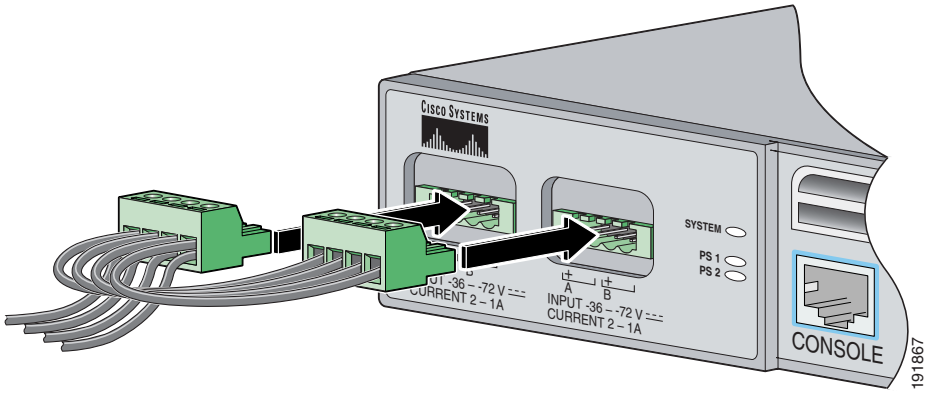
Figure 1 Connecting Separate Feeds to Each of the DC Power Terminal Blocks



1	Primary power feed	**2**	Secondary (redundant) power feed

If you want to receive an alert if an external power supply fails, do not connect feeds to one terminal block and from there connect feeds to the second terminal block. (See the example in Figure 2.) This configuration provides redundant power, and the switch continues to operate if one of the external power supplies fails. However, the software does not send a message to you that an internal power supply has failed.

Figure 2 Connecting Feeds from One Terminal Block to the Second Terminal Block



Related Documentation

These documents provide complete information about the switch and are available from this Cisco.com site:

http://www.cisco.com/en/US/products/ps6580/tsd_products_support_series_home.html

You can order printed copies of documents with a DOC-xxxxxx= number from the Cisco.com sites and from the telephone numbers listed in the "Obtaining Documentation" section on page 28.

- *Cisco ME 3400 Ethernet Access Switch Software Configuration Guide* (not orderable but available on Cisco.com)
- *Cisco ME 3400 Ethernet Access Switch Command Reference* (not orderable but available on Cisco.com)
- *Cisco ME 3400 and ME 2400 Ethernet Access Switch System Message Guide* (not orderable but available on Cisco.com)
- *Cisco ME 3400 Ethernet Access Switch Hardware Installation Guide* (not orderable but available on Cisco.com)
- *Cisco ME 3400 and ME 2400 Ethernet Access Switches Getting Started Guide (*order number DOC-7817050=)
- *Regulatory Compliance and Safety Information for the Cisco ME 3400 and ME 2400 Ethernet Access Switches* (order number DOC-7817051)
- *Configuration Notes for the Cisco ME 3400G-12CS Ethernet Access Switch* (not orderable but available on Cisco.com)
- *Cisco Small Form-Factor Pluggable Modules Installation Notes* (order number DOC-7815160=)
- *Cisco CWDM GBIC and CWDM SFP Installation Note* (not orderable but available on Cisco.com)

These compatability matrix documents are available from this Cisco.com site:

http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

- *Cisco Gigabit Ethernet Transceiver Modules Compatibility Matrix* (not orderable but available on Cisco.com)
- *Cisco 100-Megabit Ethernet SFP Modules Compatibility Matrix* (not orderable but available on Cisco.com)
- *Cisco Small Form-Factor Pluggable Modules Compatibility Matrix* (not orderable but available on Cisco.com)
- *Cisco CWDM SFP Transceiver Compatibility Matrix* (not orderable but available on Cisco.com)
- *Compatibility Matrix for 1000BASE-T Small Form-Factor Pluggable Modules* (not orderable but available on Cisco.com)

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

http://www.cisco.com/univercd/home/home.htm

The Product Documentation DVD is created monthly and is released in the middle of the month. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

If you do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Technical Support & Documentation site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. (To register as a Cisco.com user, go to this URL: http://tools.cisco.com/RPF/register/register.do) Registered users can access the tool at this URL: http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the **Cisco Product Identification Tool** to locate your product serial number before submitting a request for service online or by phone. You can access this tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Tip Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing F5.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. On the Cisco.com home page, click the **Advanced Search** link under the Search box and then click the **Technical Support & Documentation**.radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411
Australia: 1 800 805 227
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is "down" or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the magazine for Cisco networking professionals. Each quarter, *Packet* delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can subscribe to *Packet* magazine at this URL:

  http://www.cisco.com/packet

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- "What's New in Cisco Documentation" is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of "What's New in Cisco Documentation" at this URL:

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.